REMARKS

This Preliminary Amendment is filed to insert headings to conform the application to U.S. practice, to eliminate the use of multiple dependent claims, and to correct informalities in the specification, claims and abstract resulting from a literal translation of the French text.

Early action on the merits is earnestly solicited.

Respectfully submitted,

MILES & STOCKBRIDGE P.C.

Date: December 20, 2000

By: Edward J. Kondracki
Registration No. 20,604

1751 Pinnacle Drive – Suite 500
McLean, VA 22102-3833
Tel.: 703/903-9000
Fax: 703/610-8686

09/926240
PCT/EP00/02460

09/720085
JC01 Rec'd PCT/PTO 20 DEC 2000

T2146-906752-US 3797/BC(PCT)

IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (D.O./E.O./US)

Applicant: Louis GOUBIN et al.

International Application No.: PCT/FR00/01047

International Filing Date: 20 April 2000

U.S. Serial No.: To be Assigned

U.S. Filing Date: December 20, 2000

For: **SIGNATURE VERIFICATION AND AUTHENTICATION METHOD**

McLean, Virginia

PROPOSED DRAWING CORRECTIONS

Hon. Commissioner of Patents and Trademarks
Washington, D.C. 20231

Sir:

Applicant requests approval of the drawing corrections on Figs. 1 – 3B as shown in red on the attached three (3) sheets.

The proposed corrections only comprise translating the French terms into English and removing the headings "1/3" – "3/3" to conform the drawings to U.S. practice.

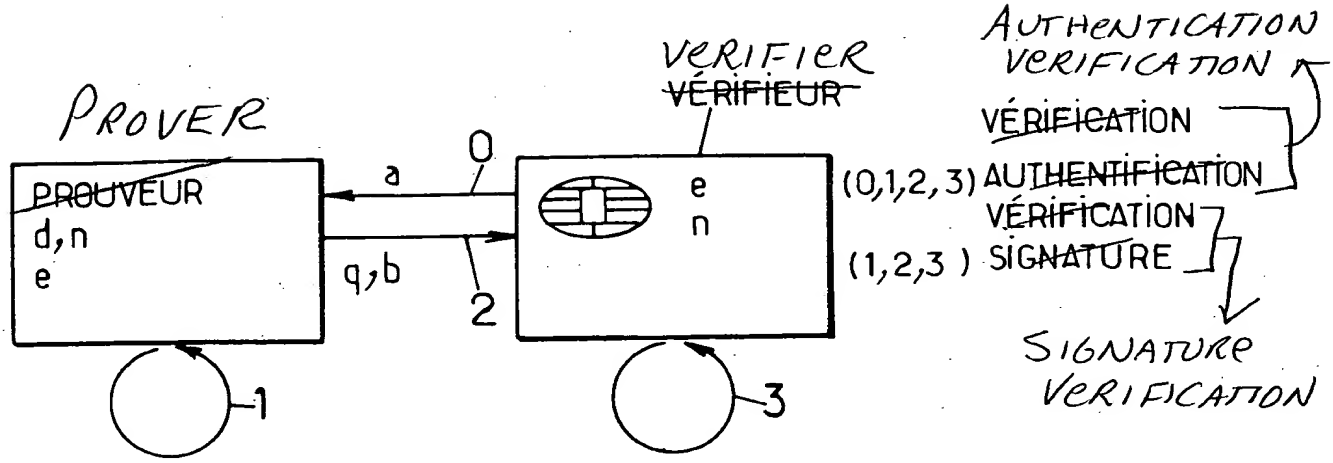
Respectfully submitted,

MILES & STOCKBRIDGE P.C.

Date: December 20, 2000

By: _____
Edward J. Kondracki
Registration No. 20,604

1751 Pinnacle Drive – Suite 500
McLean, VA 22102-3833
Tel.: 703/903-9000
Fax: 703/610-8686



$q = a * b / n$

$b = \begin{cases} a^d \bmod n & \text{si (0,1,2,3)} \\ S = Sd(M) & \text{si (1,2,3)} \end{cases}$

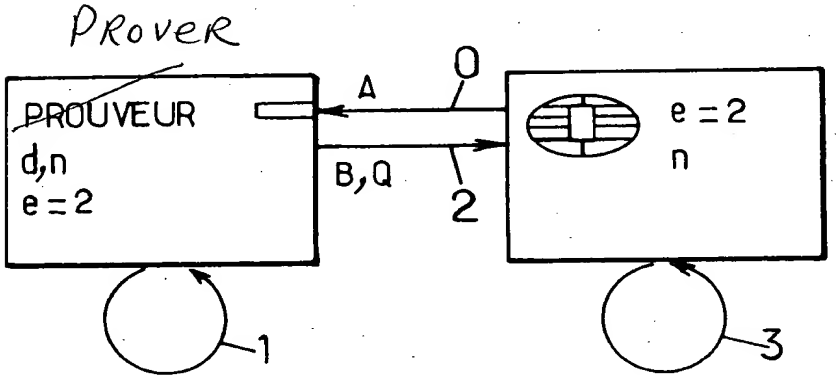
if

$a * b$

$q * n$

$a * b - q * n$

FIG.1.



$R = B = A^d \bmod n$

$Q = B * B / n$

$D_{AR} = B * B - Q * n$

$D_{AR} = A$

$D_{AR} = n - A$

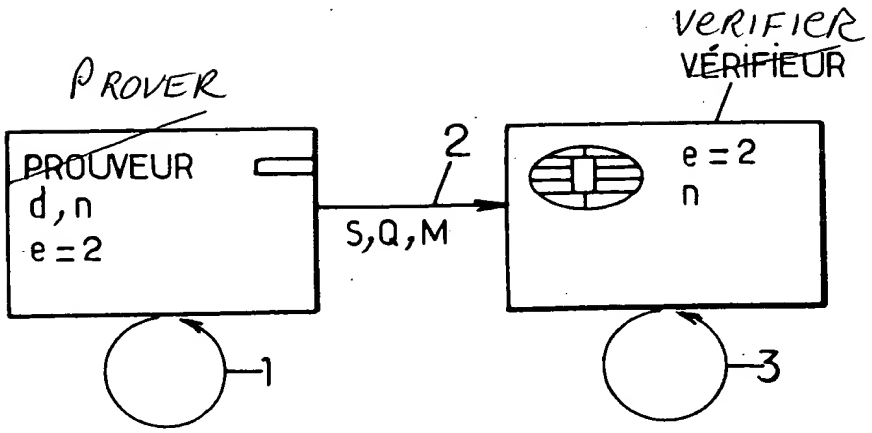
$D_{AR} = C * A \bmod n$ } $= C * A$ si $C * A < n$

$D_{AR} = -C * A \bmod n$ } $= C * A - n$ sinon

IF

IF NOT

FIG. 2a.



VÉRIFICATION
SIGNATURE SIGNATURE
VERIFICATION

$R = S = Sd(M)$

$Q = S * S / n$

$D_{SR} = S * S - Q * n$

$D_{SR} = f(M)$

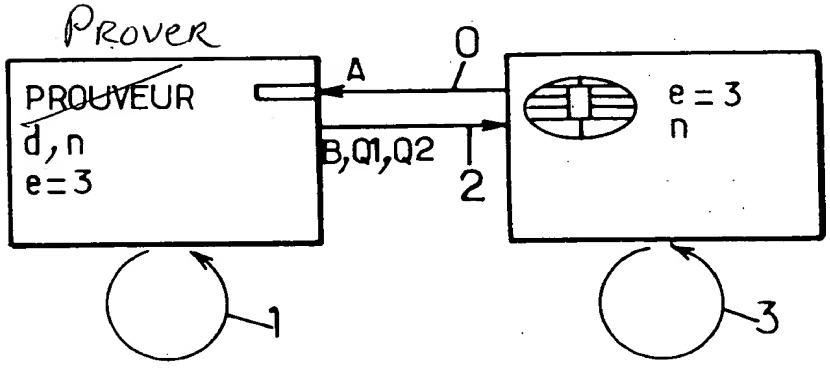
$= n - f(M)$

$= C * f(M) \bmod n = C * f(M)$ si $< n$

$= C * f(M) \bmod n = C * f(M)$ SINON

IF NOT

FIG.2b.



VÉRIFICATION
D'AUTHENTIFICATION
AUTHENTICATION
VERIFICATION

$R = B = A^d \bmod n$

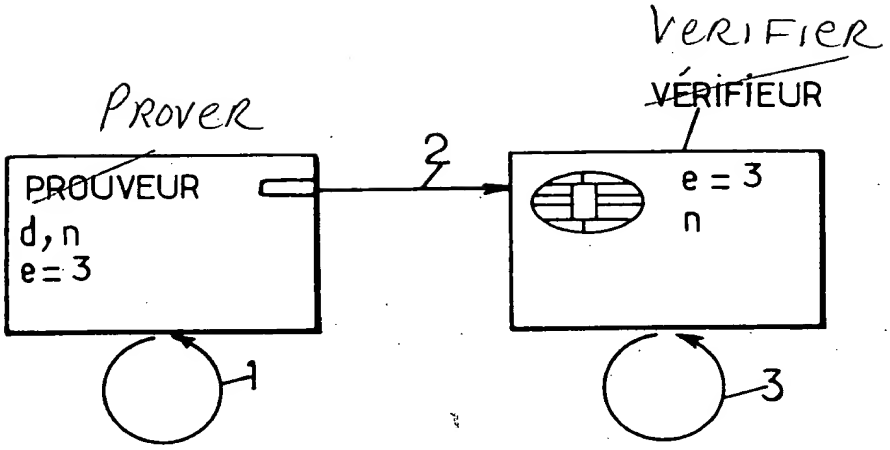
$Q1 = B * B / n$

$Q2 = B(B * B - Q1 * n) / n$

$D_{ARSA} = B(B * B - Q1 * n) - Q2 * n$

$D_{ARSA} = f(A) = A$

FIG.3a.



R = S = Sd (M)

Q1 = S * S / n

Q2 = S (S * S - Q1 * n) / n

$D_{SRSA} = S(S * S - Q1 * n) - Q2 * n$

$D_{SRSA} = f(M)$.

FIG.3b.